Dubner's Primes

Searching for twin primes and other denizens of the number world

By IVARS PETERSON

Harvey Dubner has a way with numbers—prime numbers, to be exact. Using four souped-up personal computers at his own home and two more at his son's house, he searches for titanic primes, each one running to 1,000 digits or more.

Defined as whole numbers exactly divisible only by themselves and one, prime numbers have long fascinated both professional and amateur mathematicians. They raise intriguing questions: Is there a formula or a simple rule that generates only primes? Is there a straightforward, efficient way of checking whether a given number is prime? Do prime numbers have hidden regularities that belie the apparent unevenness evident in the sequence of primes?

A semiretired electrical engineer and computer systems designer who runs Dubner International, Inc., a Westwood, N.J.-based consulting firm, Dubner has always liked number theory. But he didn't become heavily involved with prime numbers until around 1980, when personal computers for the home became available. By 1984, with the addition of special circuit boards to his machines, Dubner had more computing power for dealing with computations involving large numbers than anyone else except those with access to supercomputers.

He was also well on his way toward dominating a list of the largest known primes, now maintained by Chris K. Caldwell of the University of Tennessee at Martin. This table of all known primes with 1,000 or more digits currently has 4,590 entries.

Dubner has found more than half of the entries having more than 2,000 digits. He even has captured 17 of the 66 known primes with more than 10,000 digits, prime-number territory generally ruled by supercomputers.

"I look for big numbers," Dubner says proudly. "And it's nice to hold records." Recently, he found the largest known twin primes — a pair of primes that differ by only 2. Each of these numbers, $1,692,923,232 \times 10^{4020} \pm 1$, has 4,030 digits.

Now Dubner wants to interest mathematicians in taking advantage of the same hardware — dubbed the PC Cruncher — that speeds his own pursuits of huge primes. "I want to get this into the number theory community," he says. "Not only do you end up with a powerful computer, but it also lets you try things and leads you in directions you couldn't possibly have considered without it."

Dubner follows in the footsteps of mathematicians who have adapted computers to the special needs of number theory. Derrick H. Lehmer, a pioneer of computational number theory who died in 1991, designed and built several machines for this purpose. His creations include a remarkable photoelectric device built in 1932 for factoring numbers. A different, electronic version of this machine, built in the 1960s, is now in the Computer Museum in Boston.

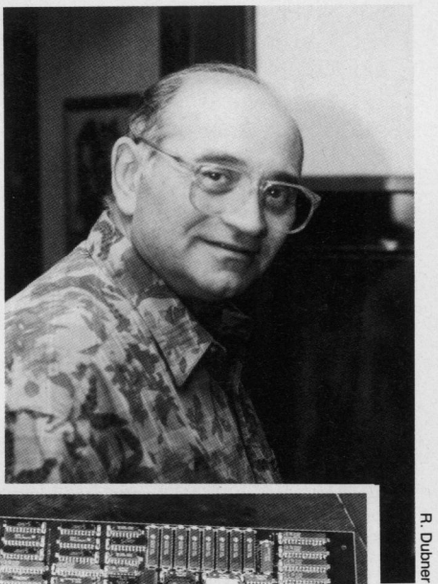
These and other computers provide the numerical raw material for testing conjectures in number theory, for discovering patterns leading to new theorems and conjectures, and for suggesting alternative approaches to long-standing problems. "Although [the computer] doesn't give you a proof, it helps you out," says Hugh C. Williams of the University of Manitoba in Winnipeg. "It provides you with ideas."

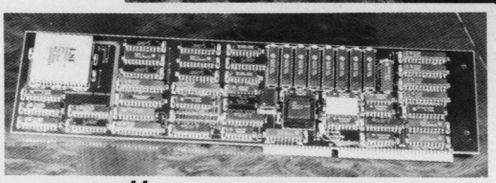
Practitioners also have a lot of fun messing with the peculiarities of prime numbers, such as their distribution. "It's interesting that you can make simple predictions about how many prime numbers there should be in various places," Caldwell says. "But they don't always go according to plan. There's a lot of randomness there."

Dubner teamed up with his son Robert, an electronic design engineer, to create the hardware needed for his prime-number searches. "My son builds the special-purpose hardware and writes the system software," Dubner says. "I program the computer and look for big primes."

The Dubner PC Cruncher is a circuit board that plugs into one of the slots available inside practically any computer that uses 80386 or 80486 microprocessor chips. The latest version of the board makes a 486 computer about 100 times faster for number theory work than its numerically unendowed counterpart.

Dubner sells the Cruncher for $2,500, which barely covers the cost of parts, let alone the software that accompanies the board. "It's a pretty useful device," says Williams, who recently purchased one. "Often when you buy things like this, they don't work. But we just plopped the thing in and right away it was working."





R. Dubner

Harvey Dubner and his PC Cruncher.

Williams already has plans for using his enhanced personal computer to look for certain kinds of numbers. "The nice thing is that you can use the machine as much as you like," he says. "You've got nobody from the computer center breathing down your neck saying they want the computer for something else."

Meanwhile, Dubner continues his never-ending search. He already has more than 20 professional papers to his credit, either as author or coauthor. His list of prime-number trophies includes a host of curios: the largest known prime whose digits are also primes; the largest known prime with one 5 and all the rest 9s; and the largest known prime whose digits are either 0 or 1.

While his computers relentlessly toil away 24 hours a day, day after day, on their latest quest, Dubner is already pondering his next set of targets in the vast territory of huge prime numbers. It may be the Sophie Germain primes, named for a French mathematician of the late 18th and early 19th centuries. While she was working on Fermat's last theorem, Germain became interested in special pairs of primes such that if p is a prime, then $2p + 1$ is also a prime. One example of such a pair is 11 and 23. Dubner wants to find a record-breaking Sophie Germain prime in the 4,000-digit range.

"Little guys with special hardware can compete with supercomputers," Caldwell remarks. "When you consider how little time an average person can get on a Cray [supercomputer], you can do very well running Crunchers 24 hours a day." □